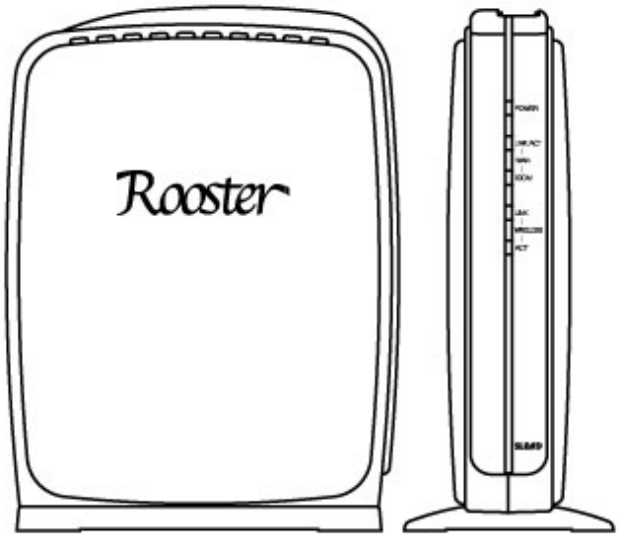
Rooster™-RW Pro

取扱説明書



http://www.sun-denshi.co.jp/sc

本機をお使いになる前に、必ず本書をよくお読みになってから設定を行ってください。

警告および注意を必ず守り、正しくお使いください。

Rooster™-RW Pro

取扱説明書 目次

- **はじめに.....1**
- **安全上のご注意(必ずお守りください。).....2**

1. Rooster-RW Pro の導入 6

1-1 主な特長.....6
1-2 Rooster-RW Pro 設定フロー.....7
1-3 同梱品の確認.....7
1-4 各部の名称と機能.....8

2. Rooster-RW Pro の導入 9

2-1 Rooster-RW Pro の接続方法.....9
2.1.1 必要な環境.....9
2.1.2 接続方法.....9
2-2 ご利用環境の確認.....9
2-3 パソコンの設定(TCP/IP の設定等).....10
2.3.1 DHCP を使用する設定(Windows XP の場合).....10

3. Rooster-RW Pro 基本設定 13

3-1 設定ツールへのログイン方法.....13
3-2 設定.....13
3-3 アドレス解決.....14
3-4 モバイルカード.....16
3.4.1 基本設定.....17
3.4.2 RAS 機能でのネットワーク構成.....18
3.4.3 対応機種/対応通信モード一覧(2008 年 4 月現在).....19
3-5 ツール.....20
3.5.1 管理者パスワードの変更.....20
3.5.2 工場出荷時の設定に戻す.....21
3.5.3 ファームウェアのアップグレード.....21
3-6 ステータス.....21
3-7 DHCP.....22
3.7.1 DHCP サーバの設定.....23
3.7.2 DHCP テーブルの表示.....23
3-8 ログ.....23
3.8.1 パケットログの参照.....24
3.8.2 モバイルカードログの参照.....25
3.8.3 アドレス解決ログ.....26
3.8.4 WAN ハートビートログ.....27
3-9 統計.....27

4. Rooster-RW Pro の高度な設定..... 28

4-1 基本設定と高度な設定を切り替える.....28
4-2 仮想(バーチャル)サーバの設定.....28
4.2.1 仮想(バーチャル)サーバとしてネットワーク上の PC の設定.....28
4.2.2 仮想(バーチャル)サーバの削除.....29
4-3 フィルタリングの設定.....29
4.3.1 フィルタの設定.....29
4.3.2 プライベート MAC フィルタリングの設定.....30
4.3.3 フィルタオプションの追加設定.....30
4.3.4 フィルタの削除.....31
4-4 特別なアプリケーションの設定.....31
4.4.1 一般的なアプリケーションを設定する.....31
4.4.2 手動で特別なアプリケーションを設定.....32
4.4.3 特別なアプリケーションの削除.....32
4-5 DMZ(LAN ポートを仮想 DMZ ポート化する場合)の設定.....32
4.5.1 DMZ ホストとしての設定.....32
4.5.2 DMZ ホストの削除.....33
4-6 MAC アドレスの変更.....33
4-7 電源制御.....33

- **資料1 ..... 35**
- **資料 2..... 36**
- **資料 3..... 38**
- **製品仕様 40**
- **外形寸法 42**

- **サポートのご案内 42**

はじめに

表記について

本取扱説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しております。

⚠警告	人体に危険を及ぼしたり、装置に大きなダメージを与えたりする可能性があることを示しています。必ずお守りください。
ⓘ注意	機能停止を招いたり、各種データを消してしまったりする可能性があることを示しています。十分に注意してください。
☼メモ	関連情報です。参考にお読みください。

商標について

「Rooster」「Sun Communications」は、サン電子株式会社の登録商標および商標登録出願中です。
その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。
本文中の各社の商標または登録商標には、TM、®マークは表示しておりません。

安全上のご注意(必ずお守りください。)

ここに記載している注意事項は、安全に関わる重要な内容ですので、必ず守ってください。本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。

	この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。
	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関する拡大損害を示しています。
	禁止行為(してはいけないこと)を示しています。
	強制行為(必ずしなければいけないこと)を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

安全上のご注意(必ずお守りください。)

⚠警告

分解禁止	本製品を分解したり、改造したりしないでください。 ⇒感電、火災、故障の原因になります。
禁止	近くに雷が発生したときには、AC アダプタをコンセントから抜いてご使用をお控えください。 ⇒落雷が火災、感電、故障の原因となるときがあります。
禁止	本製品に水などの液体をかけたり、異物を入れたりしないでください。⇒感電や火災の原因になります。 万一、本製品に液体がかかったり、異物が入ったりした場合は、AC アダプタをコンセントから抜いて、点検修理を依頼してください。
強制	製品から煙、異臭、異常音が発生した場合は、AC アダプタをコンセントから抜き、本製品を接続している機器からケーブルを取り外してください。また、修理、点検を依頼してください。 ⇒火災の原因になります。
禁止	電源ケーブルを傷つけないでください。 ⇒感電、火災の原因になります。
強制	AC アダプタは、AC100V コンセントに接続してください。また、本製品を設置、移動する時は、電源プラグを抜いてください。 ⇒故障、火災の原因になります。
禁止	梱包のポリ袋などは、小さいお子様の手の届く所に置かないでください。 ⇒小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。
強制	電源プラグは確実に根元まで差し込んでください。また、電源プラグとコンセントの間のほこりは、定期的(半年に一回程度)に取り除いてください。 ⇒電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。

⚠注意

禁止

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

⇒本製品の故障や破損などによって、発煙、発火、感電の原因に
なります。下記の環境には、特にご注意ください。

- 室内または製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所

禁止

同梱の AC アダプタ以外の電源を使用しないでください。

⇒他の電源を使用すると、故障、火災の原因になります。

強制

30cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

⇒そのまま使用すると、重大な事故になる可能性があります。

ご使用にあたってのお願い

- **本製品周辺で静電気的障害を発生させないでください。**

  ⇒本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。

- **本製品はていねいに取り扱ってください。**

  ⇒本製品に強いショックを与えると破損の原因になります。

- **本製品のお手入れは、電源を切った状態で行ってください。**

  ⇒誤動作や故障の原因になります。

- **本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。**

  汚れがひどい場合は、柔らかい布に台所中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。
  ⇒揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。

地球環境保全のため、次のことにご協力ください。

本製品および付属品は、不燃物として処分してください。廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。一般ごみとして、家庭で焼却処分しないでください。ダイオキシンや塩化水素ガスなどが発生し、環境や人体に影響を与えます。

ご注意

- **本製品の仕様は国内向けになっておりますので、海外ではご利用になれません。**

  These products are designed for use in Japan only and cannot be used in any other countries.

- **本製品は、パソコンなどの OA 機器に使用することを目的に設計、製造されています。**

  医療機器や幹線通信機器、電算機システムなどの、きわめて高い安全性や信頼性が要求される用途には使用しないでください。

- **取扱説明書について、次の点にご注意ください。**

1. 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
2. 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
3. 本取扱説明書の内容につきましては、万全を期して作成致しましたが、万一ご不審な点や、ご不明な点、誤り、記載漏れ、その他お気づきの点等ございましたら、当社までご連絡ください。
4. 適用した結果の影響につきましては、3 項にかかわらず責任を負いかねますので、ご了承ください。
5. 本取扱説明書で指示されている内容につきましては、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害につきましては、保証期間内であっても責任を負いかねますので、ご了承ください。
6. 本取扱説明書の設定画面は開発段階のもので、実際の画面とは一部異なる部分があるかもしれません。本取扱説明書で使われている画面写真は一例としてください。

1. Rooster-RW Proの導入

1-1 主な特長

- **耐環境性能が大幅に向上**

厳しい環境化での安定した運用を行う事が出来る耐環境性能の向上を図る為、従来機種「Rooster-RW(SC-RS5FJ)」のハードウェアの全面リニューアルを行いました。「Rooster-RW(SC-RS5FJ)」のほとんどの機能を継承した上で、耐ノイズ、耐静電気性能等を大幅に向上させ、自動販売機、映像監視装置等への組み込みによる無人環境において移動体通信による安定運用を実現する各種機能を新たに搭載致しました。

- **長期間の安定運用を実現する各種電源制御機能**

ハードウェアの耐環境性能向上に加え、「モバイルデータ通信カードを24時間毎にリセットする」、「Rooster-RW Proの電源を35時間又は6日間毎にハードウェア処理で電源OFF/ONさせる」機能、「Rooster-RW Proを24時間毎にソフトウェア処理で自動電源OFF/ONさせる」機能を新たに搭載しております。

- **強力なウォッチドック機能**

従来機種「Rooster-RW(SC-RS5FJ)」で搭載されていたソフトウェアウォッチドック機能に加え、Rooster-RW Pro本体のCPUに何らかの影響を受けて正常な動作が不能になった場合には、即座に電源をOFF/ONするハードウェアウォッチドック機能を実装しております。
また、モバイルデータ通信カードが連続して12回ダイアルアップに失敗すると、モバイルデータ通信カードの障害と判断し、即座にモバイルデータ通信カードの電源のみをOFF/ONさせ復旧を図る事が可能です。

- **モバイルデータ通信カードのステータス情報表示機能**

ウィルコム社のAIR-EDGEシリーズ接続時、カードの電話番号、電界強度、位置情報（緯度、経度）を設定画面内に表示します。
設置時に電界強度や位置情報の確認が可能となります。
※Rooster-RW Proの電源投入時に取得した情報を表示します。

- **FOMA 対応の WakeOnVoice 機能**

従来機種「Rooster-RW(SC-RS5FJ)」では不可能だったFOMAカード接続時の「WakeOnVoice」機能に対応しました。
FOMAカード接続時に外部のFOMA音声端末よりAV通信モード（TV電話）での着信をトリガとして、自動ダイアルアップを行わせる事が可能となります。

- **リモートアクセス機能**

Rooster-RW ProはPHS、FOMA対応カード型端末による1回線収容のリモートアクセス機能を搭載しています。社内などイントラネット環境に設置すれば、外部からモバイルカードなどによるダイヤルアップ接続環境を構築する事が可能となります。ま不正アクセスを防ぐ高度なセキュリティとしてCLIDとPAPの認証に対応しています。

- **アドレス解決機能**

Rooster-RW Proはプロバイダへ接続する度に変化するグローバルIPアドレスを、あらかじめ設定されているメールアドレスへ通知する事が可能です。また、弊社と協業パートナー様が運営するダイナミックDNSサービスを使用することが可能です。
【「どこでもカメラ」ヴィ・インターネットオペレーションズ株式会社様】（http://www.vio.co.jp）

- **従来機種の Rooster-RW と高い互換性**

従来機種「Rooster-RW(SC-RS5FJ)」で搭載されている機能は「無線LANアクセスポイント機能」、「設定ウィザード」を除いて全て継承しております。

1-2 Rooster-RW Pro 設定フロー

Rooster-RW Proを使用してダイヤルアップ接続を行う場合、最低限2までの設定を行ってください。3の設定は、必要に応じて行ってください。

1. Rooster-RW Proの設置
   - 同梱品の確認 (☞1-3 同梱品の確認)
   - 機器の接続 (☞2-1 Rooster-RW Proの接続方法)
   - クライアントPCの設定
     (☞2-3 パソコンの設定（TCP/IPの設定等)

2. Rooster-RW Proの基本設定
   - 基本設定 (☞3-2 設定)
   - アドレス解決の設定(☞3-3アドレス解決)
   - モバイルカードの設定(☞3-4モバイルカード)

3. Rooster-RW Proの高度な設定
   - 基本設定と高度な設定画面を切り替える(☞4 Rooster-RW Proの高度な設定)
   - 仮想（バーチャル）サーバ(☞4-2仮想（バーチャル）サーバの設定)
   - フィルタリングの設定(☞4-3フィルタリングの設定)
   - 特別なアプリケーションの設定(☞4-4 特別なアプリケーションの設定)
   - DMZの設定(☞4-5 DMZ（LANポートを仮想DMZポート化する場合）の設定)
   - MACアドレスの変更(☞4-6 MACアドレスの変更)
   - 電源制御の設定(☞4-7電源制御)

1-3 同梱品の確認

パッケージには、次のものが同梱されています。
万一不足しているものがありましたら、お買い求めの販売店、もしくはサポートセンターにご連絡ください。

- Rooster-RW Pro 本体 1 台
- CD-ROM
  (本取扱説明書 収録) 1 枚
- 保証書 1 枚
- AC アダプタ 1 個
- UTP ケーブル(カテゴリ 5 ストレート) 1 本
- 縦置きスタンド 1 個
- カードスロットフタ 1 個

1-4　各部の名称と機能

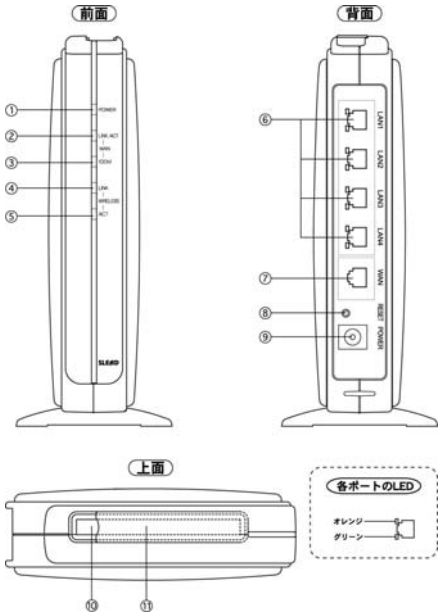


図 1-1　　Rooster-RW Pro 各部名称

1. POWER ランプ

   Rooster-RW Pro の電源が入っている場合は、グリーンの LED が点灯します。この LED が消灯している場合は Rooster-RW Pro の電源が入っていないことを表します。

2. LINK/ACT ランプ

   WAN ポートにケーブルがつながれているときに点灯します。WAN ポートにデータが流れると点滅します。

3. 100M ランプ

   WAN ポートが 100BASE で接続されると点灯します。

4. LINK ランプ

   ・モバイルカードがリンクすると点灯します。（ダイヤル中は点滅します。）
   ・設定で[モバイルカードを使用する]になっている場合で、モバイルカードが未装備、または認識されていない場合はACTランプと共に点滅します。

5. ACT ランプ

   ・モバイルカードがリンクすると点灯します。（ダイヤル中は点滅します。）
   ・設定で[モバイルカードを使用する]になっている場合で、モバイルカードが未装備、または認識されていない場合はLINKランプと共に点滅します。

6. LAN1～4 ランプ

   LAN ポートです。ローカルネットワーク側の PC もしくは HUB を接続します。
   LAN ポートの LED について

   ・グリーンLED-ケーブルがつながれているときに点灯し、データが流れると点滅します。
   ・オレンジLED-100BASEで接続されると点灯します。

7. WAN

   WAN ポートです。ブロードバンドネットワーク プロバイダに接続する ADSL モデムやケーブルモデムを接続します。モバイルカードと同時に使用することはできません。

8. RESET スイッチ

   Rooster-RW Pro を工場出荷時の設定に戻します。工場出荷時の設定に戻すには、スイッチを針金などで手ごたえのある位置まで、6 秒以上押し続けてください。

9. POWER

   付属している AC アダプタのコネクタを接続するジャックです。

10. カード取り出しボタン

    Rooster-RW Pro からカードを取り出すときに押すボタンです。

11. カード差し込み口

    Rooster-RW Pro へカードの挿入口です。

2. Rooster-RW Proの導入

2-1 Rooster-RW Proの接続方法

2.1.1 必要な環境

- TCP/IP が利用できる OS(Windows、MacOS、各種 UNIX など)を搭載し、Ethernet ポートを搭載したパソコン
- LAN（UTP）ケーブル
- ブロードバンド回線（ブロードバンドルータとして使用する場合）
- モバイルカード（AIR-EDGE 又は FOMA、b-mobile、CDMA 1X WIN カード、ソフトバンクモバイルカードを使用する場合）
- Internet Explorer 6.0 以上のブラウザ
  (上記以外のブラウザでは、正常に動作しない可能性があります。)

2.1.2 接続方法

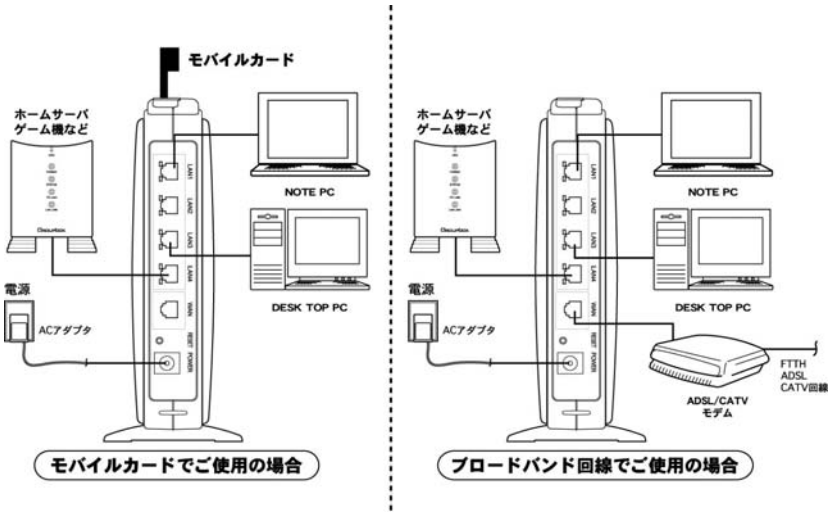


図 2-1　　Rooster-RW Pro 接続図

1. Rooster-RW Pro とパソコンの電源が入っていないことを確認してください。
2. LAN ポートにクライアントとなるパソコンを接続してください。
3. モバイルカードを接続してください。
4. Rooster-RW Pro に AC アダプタの電源コネクタを接続してください。
   次に AC アダプタをコンセントに接続してください。
5. パソコンの電源を入れてください。

注意

モバイルカードは、必ず電源を切った状態でカードの抜き差しを行ってください。電源を入れた状態でカードの抜き差しを行うと、Rooster-RW Pro が作動しません。

AC アダプタは、必ず付属のものを使用してください。
付属の AC アダプタ以外を使用すると、故障・誤作動の原因になります。
付属の AC アダプタ以外を使用された場合の故障は、保証対象外となりますのでご了承願います。

2-2 ご利用環境の確認

Rooster-RW Proとパソコンを接続するためにはパソコンにLAN環境が必要です。
LAN環境が無い場合には、ご利用のパソコンにあわせてLAN機器をご用意ください。

- デスクトップパソコンで LAN ポートが標準で装備されていない場合、LAN ボードをご利用のパソコンにあわせて増設してください。
- ノートパソコンで LAN ポートが標準で装備されていない場合、LAN カードをご利用のパソコンにあわせて増設してください。

インターネット接続の場合
通信事業者との契約が完了している必要があります。以下についてご確認願います。

- モバイルカード等の回線事業者との契約、工事が完了している必要があります。
  （(株)NTT ドコモ、(株)ウィルコムなど）
- インターネット接続サービスであるプロバイダへの契約の完了している必要があります。（OCN、@nifty 等)
  事業者によっては回線事業者とプロバイダが同じ契約の場合があります。
  その場合別途プロバイダへの契約は必要ありません。

- Rooster-RW Pro の設定には、以下の情報が必要になります。プロバイダとの契約時に提供されている情報をご用意ください。不明な場合はご契約のプロバイダへお問い合わせください。

■ **PPPoE の場合（フレッツ等）**

ユーザ名、パスワード。

■ **DHCP をご利用の場合（YahooBB 等）**

コンピュータ名、DNSサーバのIPアドレス。（プロバイダ指定の場合）

■ **固定 IP アドレスで接続の場合**

WAN側のIPアドレス、サブネットマスク、ゲートウェイIPアドレス。

■ **モバイルカードをご利用の場合**

アクセスポイントへの電話番号、ユーザ名、パスワード。

RASとして使用する場合

- モバイルカード等の回線事業者との契約、工事が完了している必要があります。
（(株)NTT ドコモ、(株)ウィルコムなど）

注意

回線事業者（プロバイダ）によってはルータを使ってのインターネットアクセスを禁止している場合があります。事前にご確認ください。

LAN 型 PPPoE 接続（un numbered 接続）には対応しておりません。

回線事業者（プロバイダ）によっては、ADSL/ケーブルモデムに接続する機器のMACアドレスの申請が必要な場合があります。その場合は本製品のMACアドレスを確認してください。確認方法は(☞4-6MACアドレスの変更)を参照してください。

2-3　パソコンの設定（TCP/IPの設定等）

Rooster-RW Proにアクセスできるように、クライアントパソコンにDHCPクライアントの設定をします。
DHCPを使用しない場合は、各パソコンに手動でIPを設定する必要があります。その方法は、ネットワークカード及びWindowsのマニュアル等をご覧ください。

2.3.1　DHCPを使用する設定（Windows XPの場合）

1. コンピュータ管理者または同等の権限のユーザ名でログオンしてください。
2. コントロールパネルを開き、[ネットワークとダイヤルアップ接続]を選び、[ネットワーク接続]をダブルクリックして開きます。
(クラシック表示の場合は、コントロールパネルを開いた後、[ネットワーク接続]のアイコンをクリックします。)

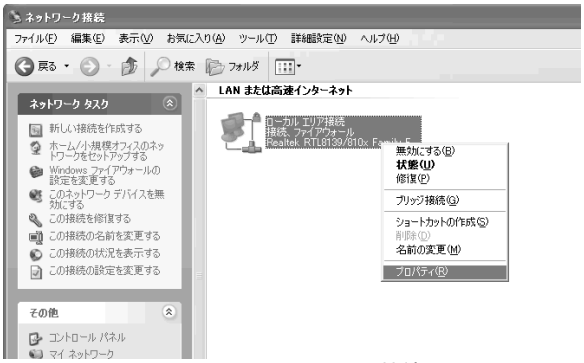


図 2-2　　ネットワーク接続

3. 「ローカルエリア接続」を右クリックし、[プロパティ]をクリックします。

ローカルエリア接続のプロパティが表示されます。

図 2-3　　ローカルエリア接続のプロパティ

4. 「インターネットプロトコル（TCP/IP）」選び、[プロパティ]をクリックします。
   TCP/IPプロパティダイアログが表示されます。
5. 「IP アドレスを自動的に取得する」、「DNS サーバのアドレスを自動的に取得する」を選択します。

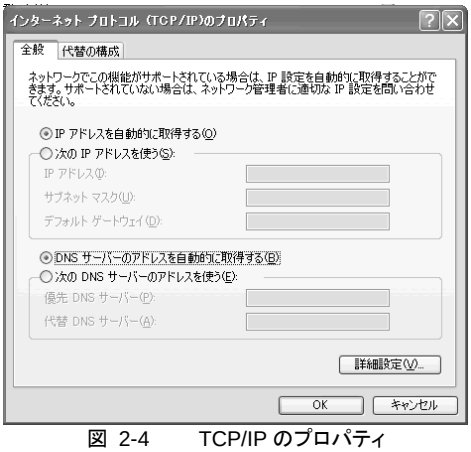


図 2-4　　TCP/IP のプロパティ

6. [OK]をクリックしてダイアログを閉じます。
   [ローカルエリア接続のプロパティ]画面も、[OK]をクリックして閉じます。

プロバイダからドメイン名の指定がされている場合のみお進みください。

7. TCP/IP 詳細設定画面の DNS タブをクリックし、DNS タブ内にある以下の DNS サフィックスを順に追加するを選択してください。

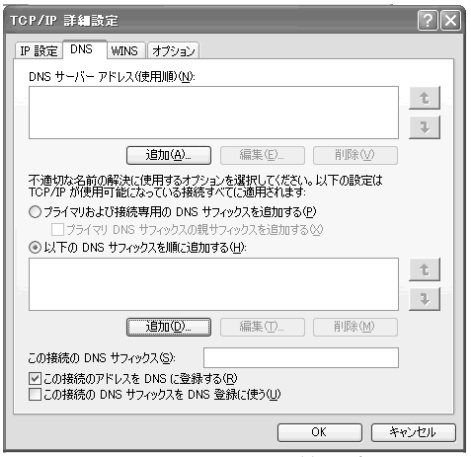


図 2-5　　TCP/IP 詳細設定

8. 追加ボタンをクリックし、プロバイダから指定されたドメイン名を入力してください。

図 2-6　　TCP/IP ドメイン サフィックス

9. [OK]をクリックして設定を完了します。

注意　複数のパソコンでインターネット接続を行う場合、全てのパソコンでネットワーク設定が必要です。

3. Rooster-RW Pro 基本設定

3-1 設定ツールへのログイン方法

1. WWW ブラウザを起動します。
2. WWW ブラウザのアドレス入力欄に、Rooster-RW Pro の LAN 側 IP アドレス「**http://192.168.62.1/**」(工場出荷時状態)を入力し、Enter を押します。

図 3-1 Rooster-RW Pro アドレスの入力

ログインダイアログボックスが表示されます。

図 3-2 ネットワークパスワードの入力画面

3. ユーザー名に「admin」、パスワードに「1234」(工場出荷時状態)と入力した後、OK ボタンをクリックします。
4. Rooster-RW Pro ツールが表示されます。

> **注意**
>
> 設定ツールは JavaScript を使用しています。
> **ブラウザの JavaScript をオンにしてから**設定を行ってください。
>
> 設定ツールを表示し、しばらく放置すると、一旦ログアウト処理を行います。その後、設定ツールにアクセスすると、再度ログインダイアログボックスが表示されます。
>
> ここで入力するユーザー名、パスワードは、Rooster-RW Proの設定ツールにアクセスするためのもので、プロバイダから提供されるユーザー名、パスワードとは異なるものです。
> (パスワードの変更方法は、☞3-5ツールをご覧ください。)

3-2 設定

ホスト名、ドメイン名、LANのIPアドレス、WANのIPアドレス、PPPoEログインなど、本製品の基本的な設定を行います。

図 3-3 Rooster-RW Pro 設定画面

> **注意**
>
> プロバイダから配布される PPPoE 接続ソフトウェアをパソコンにインストールする必要はありません。インストールしてある場合は、ソフトウェアを無効にしてください。

1. ホスト名

   ホスト名を入力してください（オプション）。プロバイダによって、入力が必須になる場合があります。この情報がはっきりしない場合は、プロバイダに確認してください。

2. ドメイン名

   プロバイダのドメイン名を入力してください（オプション）。プロバイダによって、入力が必須になる場合があります。この情報がはっきりしない場合は、プロバイダに確認してください。

3. ファームウェアバージョン

   ファームウェアのバージョンを確認できます。
   この値は、現在使用しているファームウェアのバージョンおよび日付です。

4. LAN IP アドレス

   必要な場合は、IPアドレスを変更してください。通常は変更する必要はありません。

   注意 DHCP サーバ実行中に LAN の IP を変更するには、クライアント PC を再起動する必要があります。DHCP サーバを実行せずに LAN の IP アドレスを変更した場合は、ネットワーク内全てのクライアント PC の IP アドレスを手動で変更する必要があります。

5. WAN/RAS IP アドレス

   WANのIPアドレスについては「IPアドレスを自動取得する」か「IPアドレスを指定する」のどちらかを選択してください。IPアドレスを指定する場合はWAN IPアドレス、サブネットマスク、ゲートウェイを入力してください。これらの情報はプロバイダから提供されます。
   この設定は、WANポート（PPPoEを除く）、モバイルカードでのダイヤルアップ接続（インターネット接続）もしくはRAS接続時に使用するIPアドレスを設定します。

6. PPPoE

   PPPoEはフレッツ等を使用する時設定します。ユーザー名とパスワードを設定することにより、プロバイダがインターネットに接続することを可能にします。
   プロバイダがPPPoEを使用する場合は、「使用する」を選択し、7に進んでください。そうでなければ「使用しない」を選択し、8に進んでください。

   警告 PPPoE を使用する場合は、ネットワーク上にある全てのパソコンの PPPoE 接続を解除してください。PPPoE とモバイルカードは併用できません。

7. PPPoE を使用する場合は、PPPoE ユーザー名とパスワードを入力してください。

8. WAN ハートビート

   必要な場合、WANハートビートを設定してください。この機能はWANの接続状態を逐次チェックするために使用します。WANハートビート機能を使用する場合は「使用する」を選択してください。使用しない場合は「使用しない」を設定し、11へ進んでください。

9. WAN ハートビートを使用する場合は監視時間を入力してください。設定された時間毎に WAN ゲートウェイへの接続状態を PING にて確認します。

   警告 AIR-EDGE カード、CDMA 1X WIN カードでは WAN ゲートウェイが PING に反応しないため、この機能は使用できません。また、ネットワークシステムによっては同様に使用できない場合がございます。

10. WAN ハートビートで WAN への接続確認に失敗した場合の動作を設定してください。失敗が連続した時（10 回）に本機をリセットすることが出来ます。その場合「無応答が連続して発生した場合、本機をリセットする」を選択してください。ログのみを残す場合「ログに記録する」を選択してください。

11. 選択した設定で良ければ 設定 ボタンをクリックして、完了します。また、 キャンセル ボタンをクリックすることで設定を中止することが出来ます。

3-3 アドレス解決

外部ネットワークからRooster-RW Proに接続する場合、Rooster-RW Proに割り当てられたグローバルIPアドレスを知っておく必要がありますが、通常のプロバイダ契約ではインターネットに接続する度にグローバルIPアドレスが任意に変化してしまいます。外部の相手から接続できるようこの問題を解決するには、この設定を行います。

図 3-4　　アドレス解決設定画面

1. 基本設定

   アドレス解決機能を使用する場合、「使用する」を選択してください。使用しない場合は「使用しない」を選択し、7に進んでください。

2. アドレス解決を行うためにサービスを選択します。

■ **メール送信（POP before SMTP）**

メールにてグローバル IP アドレスを通知する場合に使用します。プロバイダのメールサーバ（もしくは使用するメールサーバ）が POP before SMTP 対応の場合、これを選択します。

■ **メール送信（ユーザ認証 SMTP）**

メールにてグローバル IP アドレスを通知する場合に使用します。プロバイダのメールサーバ（もしくは使用するメールサーバ）がユーザ認証 SMTP の場合、これを選択します。

■ **どこでもカメラ**

別途ご契約を行う必要があります。
ヴィ・インターネットオペレーションズ株式会社　http://www.vio.co.jp

■ **DynDns.com**

Dynamic DNS Network Service http://www.dyndns.com

DynDns.org サービスはできる限り試用でのみお使いいただくことをお勧めします。長期間に及ぶ運用用途でのご使用の場合は十分に動作検証を行ってください。恐れ入りますが、弊社ではこの場合の動作保証及び責任につきましては一切負いかねます。ご了承ください。

■ **suncomm.DDNS**

http://www.sun-denshi.co.jp/sc/ddns/index.html

弊社が運用する有償でのダイナミック DNS サービスです。別途、ご契約が必要となりますので、上記 URL をご参照ください。また、「suncomm.DDNS」機能を利用して、お客様独自にダイナミック DNS サーバを設置・運用いただくことも可能です。
「suncomm.DDNS」のプロトコル仕様につきましては、機密保持契約成立後、開示させていただきます。なお、本件は法人のお客様に限らせていただきます。

3. 各種サービスの設定を行います。

■ **メール送信（POP before SMTP）の場合**

・使用する SMTP サーバ名、POP3サーバ名を入力してください。

・使用する POP3 のアカウント名、パスワードを入力してください。

・送信先メールアドレスに、グローバル IP アドレスを通知するメールアドレスを入力してください。

・送信元メールアドレスに、送信するメールの送信者となるメールアドレスを入力してください。（入力しない場合、メールサーバによってはメールが送信されない場合があります）

■ **メール送信（ユーザ認証 SMTP）の場合**

・使用する SMTP サーバ名を入力してください。

・SMTP サーバのアカウント名、パスワードを入力してください。

・送信元メールアドレスに、送信するメールの送信者となるメールアドレスを入力してください。（入力しない場合、メールサーバによってはメールが送信されない場合があります）

■ **どこでもカメラ、DynDns.org、SunComm DDNS の場合**

契約したときに指定される DDNS サーバ名、アカウント名、パスワード、ホスト名を入力してください。

4. メール送信を指定にした場合、メール送信のメッセージ内容を設定してください。独自に指定する場合は「指定のメッセージを送信する」を選択してください。標準のメッセージを使用する場合「標準のメッセージを使用する」を選択し、6 に進んでください。標準メッセージは、以下のような形式となります。
   <例>

   タイトル　:Rooster IP Report
   送信者　:Rooster(004053010203)<from@mailaddress>
   ⇒( )内は Rooster-RW Pro の MAC アドレス
   内容　:Rooster IP-Address Report v0.00.
   MAC=004053010203 ⇒Rooster-RW Pro の MAC アドレス
   IP=10.20.30.40 ⇒割り当てられているグローバル IP アドレス

5. メール送信で指定のメッセージを送信する場合、指定のメッセージを入力します。

   〈例〉
   設定内容:実際に送信されるメッセージ
   （割り当てられているグローバルIPアドレスが10.20.30.40の場合）
   http://%s/mobile→http://10.20.30.40/mobile

> **メモ**　指定メッセージ、設定最大文字数は 60 文字です。（送信する IP アドレスも含まれます）

6. 指定されたサービスを更新させるための更新時間を設定します。

   この設定時間毎に指定されたサーバにアクセスを行います。0を指定した場合、自動更新となりグローバルIPアドレスが変更された時のみサーバにアクセスします。設定は最小5分ですので、5分以上を設定してください。

> **警告**　メールでこの設定に 0 以外（自動更新以外）を設定した場合、設定された時間毎にメールを送ります。
> サービスのサーバの負荷低減のため、できるだけ 0 の自動更新をお使いください。

7. 選択した設定でよければ、設定 ボタンをクリックして完了します。また キャンセル ボタンをクリックすることで設定を中止する事ができます。

3-4　モバイルカード

モバイルカードでインターネットへ接続する場合、RAS機能を使用する場合、FOMA LAN接続する場合、WakeOn機能を使用する場合に設定します。ブロードバンドを使用する場合は、この機能を利用することはできません。

図 3-5　　モバイルカード画面

3.4.1 基本設定

1. モバイルカードを使用する場合「モバイルカードを使用する」を選択します。使用しない場合は「モバイルカードを使用しない」を選択し、11 に進んでください。
2. 接続方法を選択してください。

■ インターネットへ接続する場合や、ダイヤルアップを行う場合、「ダイヤルアップとして使用する」を選択してください。

■ RAS として使用する場合、「RAS として使用する」を選択してください。

■ ㈱NTT ドコモの FOMA LAN 接続でクライアントとして使用する場合、「FOMA LAN 接続する」または「LAN 接続する」を選択してください。

3. 「ダイヤルアップとして使用する」（インターネットに接続する）場合、「FOMA LAN接続する」場合は、プロバイダの電話番号を入力してください。「RASとして使用する」場合は、設定する必要はありません。
（電話番号の設定について詳しくは ☞3.4.3対応機種/対応通信モード一覧（2008 年 4 月現在） を参照ください）

> **⚠警告** 間違った電話番号や違ったパラメータを設定すると通信事業者より意図しない課金がされてしまう可能性がありますので、十分ご注意ください。

4. ユーザ名、パスワードを入力します。

■ 「ダイヤルアップとして使用する」（インターネットに接続する）場合、「FOMA LAN 接続する」場合は、プロバイダより指定されたユーザ名、パスワードを入力してください。

■ 「RAS として使用する」場合は、アクセスがあったユーザのユーザ認証をする為のユーザ名、パスワードを任意で入力してください。

5. WakeOn 機能を使用する場合「WakeOn を使用する」を選択してください。使用しない場合「WakeOn を使用しない」を選択して、8 へ進んでください。
6. WakeOn 機能で受け入れる WakeOn メッセージの種類を選択してください。

■ ㈱ウィルコムが運用する WakeOn センターからメッセージを受信する場合は「WakeOn センターからメッセージを受信する」を選択してください。

> **☼メモ** WakeOn センターを利用するには、別途㈱ウィルコムと契約する必要があります。

■ ㈱ウィルコムの端末からライトメールを受信する場合は「AIR-EDGE 端末ライトメールを受信する」を選択してください。

■ 音声着信を受け取る WakeOn Voice を使用する場合は、「音声着信を受け取る」を選択してください。

> **⚠注意** WakeOn Voice機能をご利用いただくには、モバイルカードがその機能に対応している必要があります。詳しくは☞3.4.3対応機種/対応通信モード一覧（2008 年 4 月現在）をご覧ください。
>
> FOMAカードをご利用の場合は、FOMA のテレビ電話での着信のみ WakeOnします。音声着信、一般加入電話からの着信はできません。下記の表を参照ください。

<WakeOn Voice対応表>

発信 / Rooster 側：着信	一般加入電話	携帯電話音声通話	FOMA テレビ電話
PHS	○	○	×
FOMA	×	×	○

7. メッセージに認証キーによる認証を設定する場合、認証キーを入力します。（「WakeOn センターからメッセージを受信する」、「AIR-EDGE 端末からメッセージを受信する」の場合のみ） 認証キーは、受信したメッセージの先頭文字から設定された認証キー文字数分だけ文字を比較し、一致した場合は成功となります。1 文字でも違った場合は失敗となります。認証キーは、半角英数文字のみです。

設定した認証キー	受信したメッセージ	結果	
1234	5678	×	全く一致していないため
1234	1234	○	全文字一致しているため
12	1234	○	先頭 2 文字が一致しているため
12345	1234	×	5 文字目が一致しないため

8. 電話番号認証の設定

RASとして使用の場合、もしくはWakeOnを使用の場合で、電話番号認証（CLID）を行う場合、「制限する」を選択できます。行わない場合「制限しない」を選択し、10へ進みます。

9. 電話番号の指定 ボタンをクリックすると電話番号の一覧表が表示されますので、ここに RAS 接続、WakeOn メッセージ受信を許可する電話番号を入力します。

> ☼メモ　電話番号の設定は最大 50 件まで行えます。

10. PPP の詳細な設定

    無通信監視時間は、一定時間モバイルカードで通信が行われなかった時、自動的にモバイルカード接続を切断する時間を設定します。0を入力すると無通信時間を監視しませんので、自動的には切断はしません。

> ⓘ注意　0 に設定しても、電波状態の影響による切断、プロバイダから切断された場合、Rooster-RW Pro からは積極的に再接続は行いません。再接続はLAN 側から接続要求、またはRooster-RW Pro の通信で接続の必要があった場合のみとなります。
>
> 従量制課金でご契約の場合は、必ず設定するようにしてください。

11. 選択した設定でよければ 設定 ボタンをクリックして完了します。
    また、 キャンセル ボタンをクリックすることで設定を中止する事ができます。

3.4.2　RAS機能でのネットワーク構成

RAS（Remote Access Service）は、電話回線を通じて遠隔地のネットワークにダイアルアップ接続し、そのネットワークの資源を利用する機能です。

1. NAT/ファイアウォール有の場合（デフォルト）

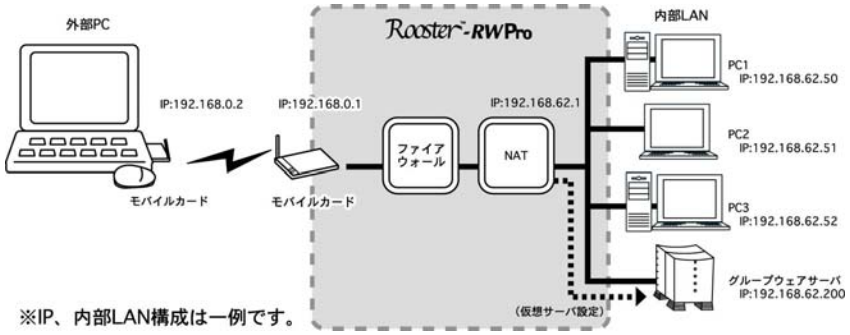


図 3-6　　構成図

> ⓘ注意　外部 PC と内部 LAN の間には NAT/ファイアウォールが入っており、外部 PC からは内部 LAN に自由にアクセスすることができません。アクセスする場合は、アクセスするマシンへ仮想サーバの設定、もしくは DMZ の設定が必要になります。
>
> 設定は☞4-2仮想（バーチャル）サーバの設定　または☞4-5DMZ（LANポートを仮想DMZポート化する場合）の設定を参照ください。

2. NAT/ファイアウォール無しの場合

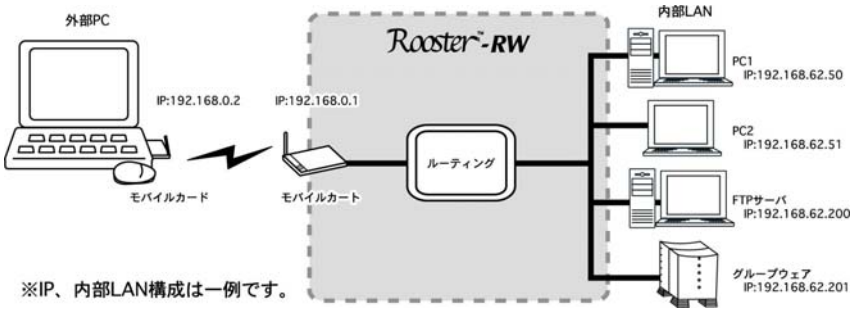


図 3-7　　構成図

外部PCと内部LANの間には通常のルーティングのみとなり、自由にアクセスすることが出来ます。外部からのアクセスセキュリティを考慮しない場合、自由度が高く、特に設定をしなくても、どのマシンへもアクセスが可能です。

注意

一般的にはRooster-RW ProのWAN側IPアドレスを固定にします。設定方法は☞3-2 設定をご覧ください。

RAS着信で使用可能なモバイルカードは、対応する一部のモバイルカードのみとなります。対応するモバイルカードは、☞3.4.3 対応機種/対応通信モード一覧（2008 年 4 月現在）をご覧ください。

3.4.3 対応機種/対応通信モード一覧（2008年4月現在）

- **対応機種一覧**

		ダイヤルアップ機能	リモートアクセス（RAS）	WakeOn	WakeOn Voice	FOMA LAN
㈱ウィルコム	CH-S203C/TD	○	○	○	―	―
	AX420S	○	○	○	○	―
	AX420N	○	○	○	―	―
	AX510N	○	○	○	―	―
	AX520N	○	○	○	―	―
	AX530IN	○	○	○	―	―
	TH-H301C	○ ※	―	―	―	―
㈱NTT ドコモ	FOMA F2402	○	○	―	○ (TV 電話)	○
	FOMA P2402	○	○	―	○ (TV 電話)	○
	FOMA P2403	○	○	―	○ (TV 電話)	○
日本通信㈱	BMH11C-J	○	―	―	―	―
	BM-H1C2-150H	○	―	―	―	―
KDDI㈱	W01K	○	―	―	―	―
	W04K	○	―	―	―	―
	W05K	○	―	―	―	―
京セラコミュニケーションシステム㈱	S101C	○	―	―	―	―
ソフトバンクモバイル㈱	VC701SI	○	―	―	―	―
	C01SI	○	―	―	―	―

※　㈱ウィルコムにお問い合わせください。

注意

上記対応機種につきましては、弊社にて動作確認済みの機種となります。

- **インターネット接続の料金コースと専用通信方式**

通信業者	ご利用の料金コース	通信方式の名称	電話番号の形式
(株)ウィルコム	つなぎ放題、[8×]、[4×]	PRO/8×/4x/パケット方式	〈電話番号〉##64
	つなぎ放題、[1×]	1x パケット方式	〈電話番号〉##61
	ネット 25、[8×]、[4×]	PRO/8×/4x/パケット方式	〈電話番号〉##64
	ネット 25	フレックスチェンジ方式	〈電話番号〉##7
(株)NTT ドコモ	FOMA	384k パケット通信	注 1) ＊99＊＊＊●#
		64k 回線交換	＊9601
KDDI(株)	CDMA 1X WIN	3.6M パケット通信	＊99＊＊24#
ソフトバンクモバイル(株)	アクセスインターネット	3.6M パケット通信	＊99#
		64k 回線交換	＊7300

注1)●は、APNの設定で登録を行ったcid番号(1-10)が入ります。
(moperaでは初期値は ”1” 、moperaUでは初期値は ”3”となります。)
mopera以外の登録を行う場合は、FOMAカードの取扱説明書等をご覧ください。
※上記の通信速度は理論値です。ご使用の環境、時間帯によって通信速度が左右されますので、予めご了承ください。

- **PIAFS 通信方式**

通信業者	通信方式	電話番号の形式
(株)ウィルコム	PIAFS 32k	〈電話番号〉##3
	PIAFS 64k	〈電話番号〉##4

注意

ブロードバンド接続（PPPoE 接続、DHCP 接続、固定 IP アドレスとの接続）との併用はできません。

電話番号の設定は、必ず接続先、通信方式をご確認の上、正しく設定を行うようにしてください。定額制でのご契約でも、専用の接続先、通信方式以外で通信を行った場合、基本料金とは別に通信料金が発生します。

パケット通信方式は、パケット通信で接続可能なプロバイダの場合のみ使用できます。
それ以外の場合は、回線交換方式で接続を行います。

パソコンにモバイルカードのドライバをインストールする必要はありません。Rooster-RW Pro が自動認識します。
ただし、モバイルカードに付属のユーティリティソフトは、Rooster-RW Pro 経由では動作致しません。

モバイルカードのサービスエリア外(圏外)では使用できません。(モバイルカードの表示ランプを確認してください。)

モバイルカードのサービスエリア内でも、電波の受信状況が悪い場合、回線が混んでいる場合などには、通信が不安定になることもあります。

3-5 ツール

ツール画面では、Rooster-RW Proの管理者パスワードの変更、設定を工場出荷時のものに戻す、ファームウェアのアップグレードを行えます。
初めてRooster-RW Proにアクセスしたときは、パスワード変更をすることを、強く推奨します。

図 3-8 ツール設定画面

3.5.1 管理者パスワードの変更

1. 古いパスワードを入力してください。工場出荷時のパスワードは「1234」です。
2. 新しいパスワードを入力してください。パスワードは 64 文字まで入力できます。
3. 確認の為、新しいパスワードを「再入力」にも入力してください。

4. 設定 をクリックすると変更され、キャンセル をクリックすると変更を元に戻せます。

> **注意**
> セキュリティのためパスワードは定期的に変更することを強く推奨します。
> 入力したパスワードはすべて「●」で表示されます。
> ユーザ名の変更はできません。「admin」のみとなります。

3.5.2 工場出荷時の設定に戻す

1. 「デフォルトの設定に戻す」を選択し、実行 ボタンをクリックしてください。警告ダイヤログが表示されます。
2. OK をクリックしてください。Rooster-RW Pro が再起動し、設定が工場出荷時の状態にリセットされます。

> **メモ**
> 設定を工場出荷時の設定に戻すには、本体裏側にある RESET スイッチを 6 秒以上長押しすることによっても可能です。

> **警告**
> 工場出荷時の設定に戻すと、ルータ全ての設定をリセットします。一旦工場出荷時の設定に戻したら、初めからルータの設定を行う必要がありますので、デフォルト設定に戻す前に、今の設定をメモしておいてください。

3.5.3 ファームウェアのアップグレード

> **メモ**
> アップデートファイルは、新しいモバイルカードへの対応、機能追加、プログラム修正などが行われるたびに、弊社ホームページにて随時公開を行う予定です。
> 下記の手順を行う前に、以下のページよりファームウェアのイメージファイルをダウンロードしてください。
> **Rooster-RW Pro 製品情報**
> http://www.sun-denshi.co.jp/sc/

1. ファームウェアのイメージファイルをウェブサイトからダウンロードし、パソコンのハードディスクに保存してください。
2. ファームウェアとパッチの場所をファームウェアのアップグレード欄に入力するか、 参照 ボタンをクリックして、ダウンロードしたアップデートプログラムデータ「＊.img」のある場所を指定します。
3. 実行 ボタンをクリックしてください。ファームウェアがアップグレードされます。

> **警告**
> ファームウェアのアップグレードには 15 秒ほどかかります。アップデート中は背面の AC アダプタを絶対に抜かないようにしてください。動作不能となる恐れがあります。
> これにより動作不能となった場合、有償修理となりますのでご注意ください。

3-6 ステータス

ステータス画面は、Rooster-RW Proのステータスを確認できます。表示されるデータは現在の設定によって変わります。

図 3-9 ステータス画面

■ **ホスト名、ドメイン名**

設定されているホスト名、ドメイン名が表示されます。

■ **PPPoE**

PPPoE 接続の現在の状態が表示されます。

■ **モバイルカード**

モバイルカードの現在の状態が表示されます。
カードが認識されると、電話番号、アンテナ強度、経度、緯度が表示されます。(接続中は、アンテナ強度、経度、緯度は表示されません。)
(モバイルカードによっては、電話番号、アンテナ強度、経度、緯度が表示されない場合があります。)

注意

モバイルカードの通信を切断する場合は 切断 ボタンをクリックすることにより可能ですが、再度インターネットに接続する場合は 接続 ボタンを押すまでモバイルカードは自動発信しません。
切断 ボタンにより回線の切断を行った後、再度通信を行う場合には 接続 ボタンをクリックするか、電源を入れなおしてください。

定額制モバイルカード以外のカードでご利用の場合はご注意ください。Two LINK DATA などの通信時間により課金される回線交換方式のモバイルカードをご利用の場合は、通信終了時に必ず 切断 ボタンをクリックして、回線を切断してください。再度通信を行う場合は 接続 ボタンをクリックしてください。

■ **LAN**

設定されている、LAN の IP アドレス、サブネットマスクが表示されます。

■ **WAN**

WAN の IP アドレス、サブネットマスク、ゲートウェイ、DNS サーバが表示されます。

■ **DHCP の開放と再取得**

設定画面で「IP アドレスを自動で取得する」と「PPPoE を使用しない」を選択し、「モバイルカードを使用しない」に設定すると、ステータス情報に「WAN ポートの DHCP を開放する」と「WAN ポートの DHCP を再取得する」のボタンが表示されます。

メモ

「WAN ポートの DHCP を開放する」や「WAN ポートの DHCP を再取得する」を選択し 実行 ボタンをクリックすると、WAN の IP アドレスを開放、再取得することが出来ます。

3-7 DHCP

DHCPサーバの設定をします。

図 3-10　DHCP 設定画面

3.7.1 DHCPサーバの設定

1. ネットワーク内に、すでにDHCP サーバが動いていないことを確認してください。また、各クライアントPC が、IP アドレスを自動に取得する設定になっていることを確認してください。
2. DHCP サーバを「使用する」を選択してください。
3. 割り当てる最初の IP を入力してください。ここで指定する IP はネットワーク上の PC に割り当てる、最初の IP アドレスになります。
4. 割り当てる最後の IP を入力してください。ここで指定する IP は、割り当てることのできる最後の IP アドレスになります。

〈例〉

開始 IP アドレスを 192.168.1.51、終了アドレスを 192.168.1.100 にした場合、DHCP サーバはネットワーククライアントに 192.168.1.51 から 192.168.1.100 までのアドレスを与えます。

5. 選択した設定で良ければ、 設定 ボタンをクリックして完了します。
   また キャンセル ボタンをクリックすることで、設定を中止することができます。

メモ Rooster-RW Pro の DHCP の設定を無効にした場合、ネットワーク上の各パソコンの IP アドレスを手動で設定する必要があります。

3.7.2 DHCPテーブルの表示

DHCPサーバによってIPアドレスを割り当てられた、現在アクティブなクライアントPCの情報を表示します。

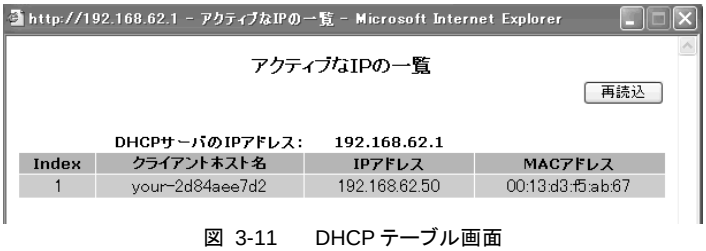


図 3-11 DHCP テーブル画面

1. DHCP テーブルの表示 ボタンをクリックすると、アクティブな IP の一覧が表示されます。
   - DHCP サーバの IP アドレス
   - インデックス番号
   - クライアントのホスト名
   - クライアントに割り当てられた IP アドレス
   - クライアントの MAC アドレス
2. 再読込 ボタンをクリックすると、表示されている情報を更新します。テーブルを見終わったらウィンドウを閉じてください。

注意 Rooster-RW Pro を再起動すると、DHCP テーブルはすべてリセットされます。

再起動後、クライアントからの IP アドレス割り当て要求を受けたタイミングで、再度 DHCP テーブルに登録されます。

3-8 ログ

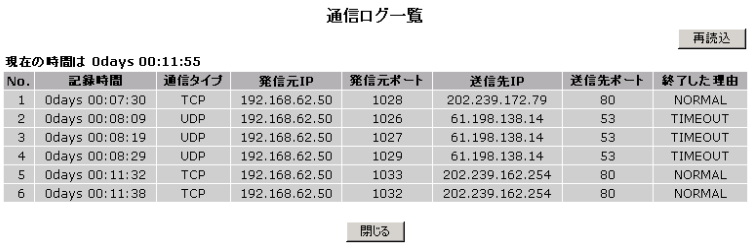
LANとWANのクライアントのアクセス履歴を記録するログファイルを確認できます。

図 3-12 ログ画面

3.8.1 パケットログの参照

■ **通信ログ**

通信ログ ボタンをクリックすると、通信ログウィンドウが表示されます。
最新のデータを見るためには、再読込 ボタンをクリックしてください。


通信ログ一覧

再読込

現在の時間は 0days 00:11:55

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	終了した理由
1	0days 00:07:30	TCP	192.168.62.50	1028	202.239.172.79	80	NORMAL
2	0days 00:08:09	UDP	192.168.62.50	1026	61.198.138.14	53	TIMEOUT
3	0days 00:08:19	UDP	192.168.62.50	1027	61.198.138.14	53	TIMEOUT
4	0days 00:08:29	UDP	192.168.62.50	1029	61.198.138.14	53	TIMEOUT
5	0days 00:11:32	TCP	192.168.62.50	1033	202.239.162.254	80	NORMAL
6	0days 00:11:38	TCP	192.168.62.50	1032	202.239.162.254	80	NORMAL

閉じる

図 3-13　通信ログ一覧画面

- No
  ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。
- 記録時間
  ログの発生した時刻が表示されます。
- 通信タイプ
  IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
- 発信元 IP アドレス
  通信の起点になる機器の IP アドレスが表示されます。
- 発信元ポート
  通信の起点になる機器の使用ポート番号が表示されます。
- 送信先 IP アドレス
  通信の宛先になる機器の IP アドレスが表示されます。
- 送信先ポート
  通信の宛先になる機器の使用ポート番号が表示されます。
- 各イベントの終了して理由
  通信が終了した理由が表示されます。

NORMAL

⇒正常に通信が行われた時に表示されます。

TIMEOUT

⇒通信セッション確立後、通信が途中で終了、あるいは終了フラグを確認できなかった時に表示されます。

■ **遮断ログ**

遮断ログ ボタンをクリックすると、遮断ログウィンドウが表示されます。
最新のデータを見るためには、再読込 ボタンをクリックしてください

遮断ログ一覧

再読込

現在の時間は 0days 00:13:34

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	終了した理由
1	0days 00:06:00	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
2	0days 00:11:21	TCP	61.240.246.46	44381	211.18.236.48	3389	Default Defense
3	0days 00:11:21	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
4	0days 00:11:57	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
5	0days 00:12:01	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
6	0days 00:12:15	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
7	0days 00:12:17	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense
8	0days 00:12:20	ICMP	192.168.62.50	ICMP	61.198.138.14	ICMP	Default Defense

閉じる

図 3-14　遮断ログ一覧画面

- No
  ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。
- 記録時間
  ログの発生した時刻が表示されます。
- 通信タイプ
  IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
- 発信元 IP アドレス
  通信の起点になる機器の IP アドレスが表示されます。
- 発信元ポート
  通信の起点になる機器の使用ポート番号が表示されます。
- 送信先 IP アドレス
  通信の宛先になる機器の IP アドレスが表示されます。
- 送信先ポート
  通信の宛先になる機器の使用ポート番号が表示されます。
- 各イベントの終了した理由
  通信が終了した理由が表示されます。

終了した理由の詳細は☞ 資料1 をご覧ください。

■ **侵入ログ**

侵入ログ ボタンをクリックすると、侵入ログウィンドウが表示されます。
最新のデータを見るためには、再読込 ボタンをクリックしてください

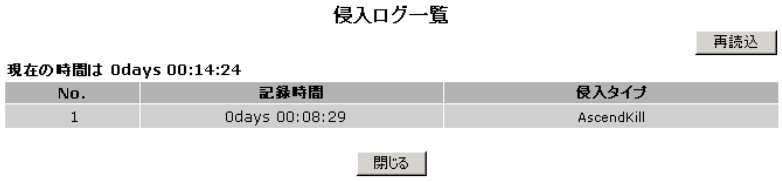


図 3-15　侵入ログ一覧画面

- No
  ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。
- 記録時間
  ログの発生した時刻が表示されます。
- 侵入タイプ
  侵入されたタイプが表示されます。

侵入タイプの詳細は☞ 資料2 をご覧ください。

3.8.2　モバイルカードログの参照

モバイルカード項目の 通信ログ ボタンをクリックすると、モバイルカードの通信情報が表示されます。

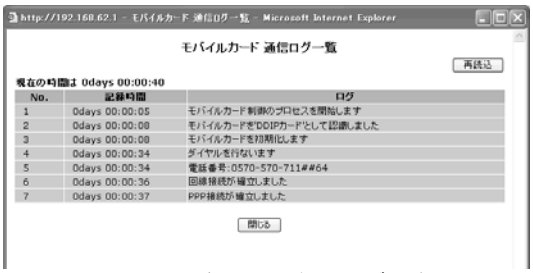


図 3-16　モバイルカード通信ログ一覧画面

- No
  ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。
- 記録時間
  ログの発生した時刻が表示されます。
- ログ
  モバイルカードの動作状態が表示されます。
  ダイヤルアップ接続、および RAS 着信接続が正常に行えない場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。

受信：NO CARRIER

回線接続の確立に失敗しました(リザルトエラー)

⇒以下のいずれかの場合が考えられます。

1. ダイヤルアップ接続先の電話番号が間違っている。
   ⇒正しい電話番号を設定してください。
2. 電波状態が悪い。
   ⇒Rooster-RW Proを通信状態のよい場所に移動するか
   (できるだけ窓側あるいは高い場所)
   あるいは、しばらく時間を置いてやり直してみてください。

受信：DELAYED

回線接続の確立に失敗しました(リザルトエラー)

⇒3 分間以内に 3 回以上、同一電話番号に電話を掛けようとすると、モバイルカードに発信規制が掛かってしまいます。
一旦接続動作を解除して、しばらくお待ちいただいてからお掛け直しください。

PPP 接続でユーザ認証に失敗しました

⇒ダイヤルアップ接続の ID、パスワードのいずれかに誤りがあります。再度、ダイヤルアップ接続の設定の確認を行ってください。

電話番号認証に登録がありません

着信条件が合わない為、無視します

⇒RAS 着信相手先リスト画面に登録されていない電話番号のため、相手からの着信要求を無視しています。RAS 着信相手先リストに該当する番号を登録するか、着番認証のチェックをオフに設定してください。

3.8.3 アドレス解決ログ

アドレス解決項目の 通信ログ ボタンをクリックすると、アドレス解決機能での通信ログが表示されます。

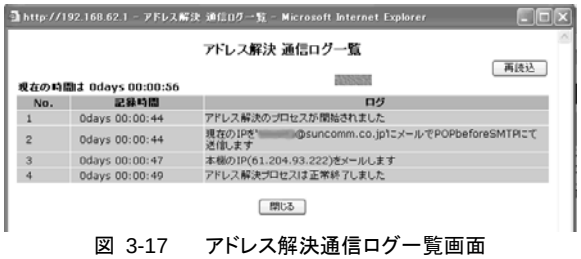


図 3-17　アドレス解決通信ログ一覧画面

- No
  ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。
- 記録時間
  ログの発生した時刻が表示されます。
- ログ
  アドレス解決機能の動作状態が表示されます。
  「アドレス解決プロセスは異常終了しました」となる場合、以下のログ表示例をご確認いただき、該当する処置をおこなってください。

- **アドレス解決をメール送信で行っている場合**

SMTP サーバ エラー : 535 Error: authentication failed

ユーザ認証 SMTP のメールサーバで、「アドレス解決」設定の、「アカウント」、「パスワード」のいずれかに誤りがある場合に表示されます。

SMTP サーバ エラー : 501 Syntax: MAIL FROM:

ユーザ認証 SMTP のメールサーバで、「アドレス解決」設定の、「送信元メールアドレス」の設定がされていないか、書式に誤りがある場合に表示されます。

SMTP サーバ エラー : 572 Relay not authorized

POP before SMTP のメールサーバで、「アドレス解決」設定の「サービスの種類」に「ユーザ認証 SMTP」の設定を行った場合に表示されます。

- **アドレス解決を DynDns で行っている場合**

DynDns サーバ エラー ：HTTP/1.1 401 Authorization Required

DynDNS 設定の、アカウント、パスワードのいずれかに誤りがある場合に表示されます。

ホスト名に誤りがある場合は表示されず、異常終了のログのみ表示されます。

3.8.4 WANハートビートログ

WANハートビート項目の 通信ログ ボタンをクリックすると、WANハートビート機能での通信結果等のログが表示されます。

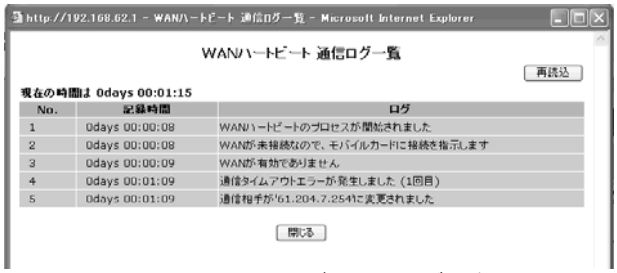


図 3-18 WAN ハートビート通信ログ一覧画面

- No
  ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。
- 記録時間
  ログの発生した時刻が表示されます。
- ログ
  WAN ハートビート機能の動作状態が表示されます。

注意 ログで表示される記録時間はログが記録された時間ですので、その事象が発生した時間と一致しない場合があります。

また、現在の時間や記録時間は、Rooster-RW Pro が起動してからの経過時間で表示されます。

再起動しますと、再起動前のログが消去されますので、ご注意ください。

3-9 統計

LAN、WANの通信状態を確認できます。

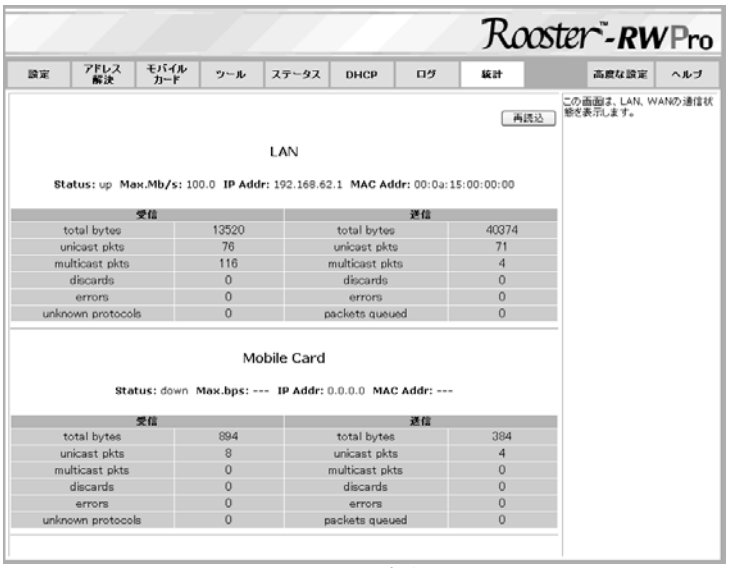


図 3-19 統計画面

- LAN

  LANの現在のステータス、最大転送速度、IPアドレス、MACアドレスの通信状態を表示します。

- WAN またはモバイルカード

  WANまたはモバイルカードの現在のステータス、最大転送速度、IPアドレス、MACアドレスの通信状態を表示します。

  最新のデータを見るためには、 再読込 ボタンをクリックしてください。ログを見終わったらウィンドウを閉じてください。

4. Rooster-RW Proの高度な設定

4-1 基本設定と高度な設定を切り替える

高度な設定には、仮想（バーチャル）サーバ、フィルタリング、特別なアプリケーション、DMZ、MACアドレスの変更、電源制御が含まれます。

1. 基本設定画面から、高度な設定の画面に切り替えるには、メニューバーの右端にある「高度な設定」タブをクリックします。
2. 一度高度な設定の画面になったらメニューバーの右端にある「基本設定」タブをクリックすることで、基本設定画面に戻れます。

4-2 仮想（バーチャル）サーバの設定

外部ネットワークからFTPやWeb等のサーバを公開するためには、仮想（バーチャル）サーバの設定が必要となります。

> ☼メモ　仮想（バーチャル）サーバを設定するとフィルタリング画面でフィルタリングが自動的に設定されます。

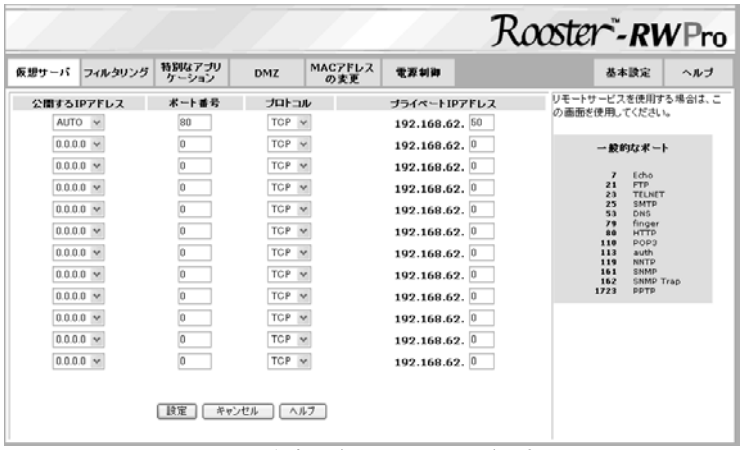


図 4-1　仮想（バーチャル）サーバ設定画面

4.2.1 仮想（バーチャル）サーバとしてネットワーク上のPCの設定

1. 公開する IP アドレスのドロップダウンリストから、IP アドレスを選択してください。WAN の IP アドレスで「IP アドレスを自動で取得する」を選択している場合、「AUTO」を選択してください。

> ⓘ注意　DMZ との併用はできません。

2. ポート番号を指定してください。指定するポート番号については、画面右の一般的なポートを参照してください。
3. ドロップダウンリストから、プロトコル（TCP、UDP、すべて）を選択してください。

> ☼メモ　プロトコルにつきましては、出来る限り、TCP または UDP を指定してください。

4. サーバ公開するパソコンのプライベート IP アドレスを指定してください。アドレスの最後の部分のみ入力します。
5. 選択した設定でよければ 設定 ボタンをクリックして完了します。
   キャンセル をクリックすることで、設定を中止することができます。

4.2.2 仮想（バーチャル）サーバの削除

仮想（バーチャル）サーバを削除するには、公開するIPアドレス欄で「0.0.0.0」を選択し、 設定 ボタンをクリックしてください。

4-3 フィルタリングの設定

ネットワークから通信するためのフィルタを設定します。Rooster-RW Proにはあらかじめいくつかのフィルタが設定されています。

警告 工場出荷時のフィルタ設定を上書きすると、ネットワーク内のクライアントPCがインターネットにアクセスできなくなる可能性があります。

新しいフィルタを定義する場合は、設定されていない列に追加することをお勧めします。

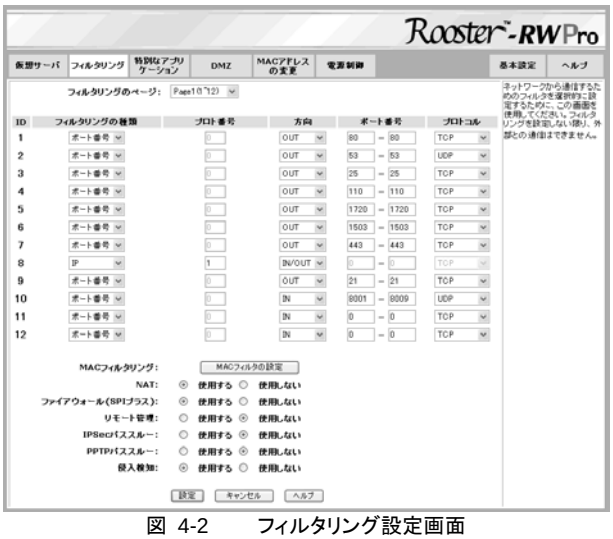


図 4-2 フィルタリング設定画面

4.3.1 フィルタの設定

1. フィルタリングのページのドロップダウンリストから表示するページ（1～12、13～24、25～36）を選択してください。

メモ 36 個までのフィルタを定義できます。

2. ドロップダウンリストから、「IP」か「ポート番号」のどちらかを選択してください。
3. IP を選択した場合、プロトコル番号（IP プロトコル番号、0～255）を入力してください。ポートフィルタリングを選択した場合、4 に進んでください。

警告 6（TCP）または 17（UDP）のプロトコル番号を入力すると、ポートフィルタリングが正しく動作しなくなります。

4. ドロップダウンリストから、IN、OUT、すべてのいずれかを選択してください。
5. 2でポートフィルタリングを選択した場合は、ポート番号（許可したいポート番号）を入力し、プロトコルのドロップダウンリストからTCP、UDP またはすべてを選択してください
6. フィルタリングの設定が終了し、設定した内容でよければ 設定 ボタンをクリックして完了します。
   キャンセル をクリックすることで、設定を中止することができます。

警告 工場出荷時の設定に加え、いくつかのフィルタはバーチャルサーバ、特別なアプリケーションを使用可能にする為に自動生成される場合があります。

デフォルト設定

ID	フィルタリング種類	プロト番号	方向	ポート範囲	プロトコル	種類
1	ポート番号	0	OUT	80-80	TCP	HTTP、インターネットアクセス
2	ポート番号	0	OUT	53-53	UDP	DNS
3	ポート番号	0	OUT	25-25	TCP	SMTP
4	ポート番号	0	OUT	110-110	TCP	POP3
5	ポート番号	0	OUT	1720-1720	TCP	NetMeeting
6	ポート番号	0	OUT	1503-1503	TCP	NetMeeting
7	ポート番号	0	OUT	443-443	TCP	SSL
8	IP	1	IN/OUT	0	0	ICMP
9	ポート番号	0	OUT	21-21	TCP	FTP
10	ポート番号	0	IN	8001-8009	UDP	Rooster 内部で使用

4.3.2 プライベートMACフィルタリングの設定

MACアドレスから、特定のパソコンがインターネットにアクセスすることを拒否できます。

1. MAC アクセスコントロールの画面を使用するため MAC フィルタの設定 ボタンをクリックしてください。

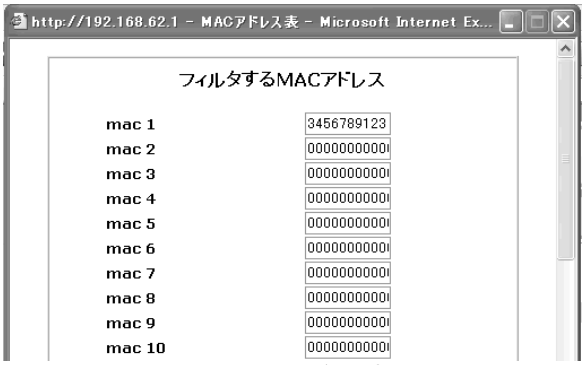


図 4-3　　MAC アドレス表の画面

> **注意**　上記の図は、MAC アドレス 10 個分のみ表示しています。

2. ブロックしたい MAC アドレスを、テーブルへ入力してください。80 個まで入力できます。
3. テーブルの下にある 設定 ボタンをクリックし、ウィンドウを閉じてください。
4. フィルタの設定が完了し、、設定した内容でよければ 設定 ボタンをクリックして完了します。
   キャンセル をクリックすることで、設定を中止することができます。

4.3.3 フィルタオプションの追加設定

リモート管理、IPsecパススルー、侵入検知といったフィルタオプションを使用することができます。

> **メモ**　これらのオプションを変更すべきかどうかわからない場合は、デフォルト設定で使用することをお勧めします。

1. それぞれのフィルタオプションで「使用する」か「使用しない」を選択してください。

■ **NAT**

この項目を有効にすると、NATの設定が可能になります。
インターネット接続を行う場合、通常は有効にします。

■ **ファイアウォール**

この項目を有効にすると、ファイアウォールを使用し、ネットワークを保護することが可能になります。

■ **リモート管理**

この項目を有効にするとWAN側からRooster-RW Proの設定ツールにアクセスできるようになります。

> **注意**　WAN 側から設定画面にアクセスする場合はポート番号 8080 を指定してください。

■ **IPsec パススルー**

この項目を有効にすると、IPsecパススルーを使用します。

> **注意**　設定後、IPsec パススルーが有効にならない場合は、別途個別にフィルタリングの設定を行ってください。
> 設定方法は☞ フィルタリングの設定 を参照ください。

■ **PPTP パススルー**

この項目を有効にすると、VPNを可能にするためPPTPを使用します。

> **注意** 設定後、PPTP パススルーが有効にならない場合は、別途個別にフィルタリングの設定を行ってください。
> 設定方法は☞ フィルタリングの設定 を参照ください。

■ **侵入検知**

この項目を有効にすると、外部からの攻撃を記録することができます。

2. 選択した設定で良ければ、 設定 ボタンをクリックして完了します。
 キャンセル をクリックすることで、設定を中止することができます。

4.3.4 フィルタの削除

フィルタリストから、既存のフィルタを削除することが出来ます。

> **注意** 工場出荷時のデフォルトのフィルタ、バーチャルサーバや特別なアプリケーションに関係するフィルタを削除すると、サービスが行えなくなる可能性があります。

1. IP フィルタの削除
 プロトコル番号に「0」を入力し、 設定 ボタンをクリックしてください。
2. ポートフィルタリングの削除
 ポート番号欄に「0」を入力し、 設定 ボタンをクリックしてください。

4-4 特別なアプリケーションの設定

この機能は、オンラインゲームやビデオ会議のようなマルチセッションアプリケーションに必要な場合があります。

> **メモ** 特別なアプリケーションの設定を行うと、フィルタが自動作成される場合があります。

図 4-4 特別なアプリケーション設定画面

> **警告** テーブルの最初の行は、FTP のためにあらかじめ作成されています。これらを上書きすると、2 つの機能が使えなくなります。
>
> FTP はパッシブモードをご利用ください。
>
> **メモ** セッションチェーンは特定のアプリケーションソフトウェアが複数のポートを使用して通信を行う場合に、それらを 1 つのセッションとして認識して、高度なパケットフィルタを実現します。TCP だけでなく、UDP パケットもセッション単位で監視します。

4.4.1 一般的なアプリケーションを設定する

1. 一般的なアプリケーションのドロップダウンリストから、適用したアプリケーションを選択してください。
2. No のドロップダウンリストから番号を選ぶことで、テーブルの特定のラインを選択してください。
3. Copy to のボタンをクリックしてください。設定されたアプリケーションがテーブルに表示されます。
4. 設定 ボタンをクリックすると、設定を変更し、 キャンセル ボタンをクリックすると設定を元に戻します。

4.4.2 手動で特別なアプリケーションを設定

手動で特別なアプリケーションの設定を行うことができますが、エキスパートなユーザが行うべきです。どの設定をするべきかわからない場合は、一般的なアプリケーションの設定を使用することをお勧めします。

1. 設定する行を選んでください。

> **メモ** 別のアプリケーションを登録するために現在の設定を上書きすると、上書きされたアプリケーションは使えなくなります。

2. ドロップダウンリストから使用するプロトコル（TCP、UDP）を選択してください。
3. ポート範囲を指定してください。
   このパラメータはアプリケーションが使用するポート番号を識別します。
4. 最大通信間隔を入力してください。
   このパラメータは動的なセッションの最大間隔をミリ秒単位で入力します。
5. セッションチェーンのドロップダウンリストから「使用する」か「使用しない」を選択してください。
6. 5 で「使用する」を選択した場合、UDP チェーンの「使用する」か「使用しない」かを選択できます。5 で「使用しない」を選択した場合は、7 へ進んでください。
7. アドレス交換のドロップダウンリストから、「使用する」か「使用しない」を選択してください。このパラメータは 2 進法のアドレス置換を行うかどうかを設定します。
8. 7 で「使用する」を選択した場合は、アドレス変換から TCP か UDP を選択することができます。7 で「使用しない」を選択した場合は、9 へ進んでください。
9. マルチホストのドロップダウンリストから「使用する」か「使用しない」を選択してください。このパラメータを有効にすると、異なる遠隔のホストから、新しいセッションを開始することを可能にします。
10. 選択した設定で良ければ、 設定 ボタンをクリックし完了します。
    キャンセル ボタンをクリックすると設定を元に戻します。

4.4.3 特別なアプリケーションの削除

特別なアプリケーションのリストから削除することができます。

1. ポート範囲に「0-0」を入力してください。
2. 設定 ボタンをクリックしてください。

4-5 DMZ（LANポートを仮想DMZポート化する場合）の設定

DMZ機能は、仮想（バーチャル）サーバ機能と同様、インターネット上（リモートホスト）から、LAN側の接続機器にアクセスを行わせる際に設定します。ポート番号が不明な時でも設定できるため、ポート番号が特定できない通信を行いたい場合などに最適な設定です。

> **警告** DMZ として設定された機器には、フィルタリングの設定が働きません。セキュリティには十分ご注意ください。

図 4-5 DMZ の設定画面

4.5.1 DMZホストとしての設定

1. 公開される IP アドレスをドロップダウンリストから選択してください。WAN の IP アドレスで「IP アドレスを自動で取得する」を選択している場合「AUTO」を選択してください。

> **メモ** 仮想（バーチャル）サーバ設定は無効になります。

2. サーバ公開するパソコンのプライベート IP アドレスを指定してください。アドレスの最後の部分のみ入力します。
3. 選択した設定でよければ 設定 ボタンをクリックして完了します。
   キャンセル をクリックすることで、設定を中止することができます。

4.5.2 DMZホストの削除

DMZホストを削除するには、公開するIPアドレスで「0.0.0.0」を選択し、 設定 ボタンをクリックしてください。

4-6 MACアドレスの変更

Rooster-RW ProのWANポートのMACアドレスを変更します。通常変更する必要はありません。プロバイダにすでにPCのMACアドレスを登録している場合、Rooster-RW ProのMACアドレスを登録済みのMACアドレスに変更することにより、プロバイダへの登録変更をしなくてもご利用いただけます。

> メモ　モバイルカードでご使用の場合は、変更する必要はありません。

図 4-6　MAC アドレスの変更画面

1. プロバイダに登録した LAN カードの MAC アドレスを使用する場合があります。

> メモ　Rooster-RW Pro に設定されている現在の WAN ポート MAC アドレスと工場出荷時の MAC アドレスが画面に表示されます。

2. WAN ポート MAC アドレスに使用する MAC アドレスを入力してください。
3. 「WAN ポートの MAC アドレスの変更」を選択すると設定を変更し、「WAN ポートの MAC アドレスを工場出荷時に値に戻す」を選択すると設定を工場出荷時に戻します。
4. 選択した設定でよければ 設定 ボタンをクリックして完了します。
   キャンセル をクリックすることで、設定を中止することができます。

> 注意　プロバイダによっては、ルータの MAC アドレスの申請が必要な場合があります。

4-7 電源制御

Rooster-RW Proおよびモバイルカードの電源の制御を行います。この機能は定期的に再起動を行うことにより、より安定したご使用をしていただくことを目的とします。

図 4-7　電源制御設定画面

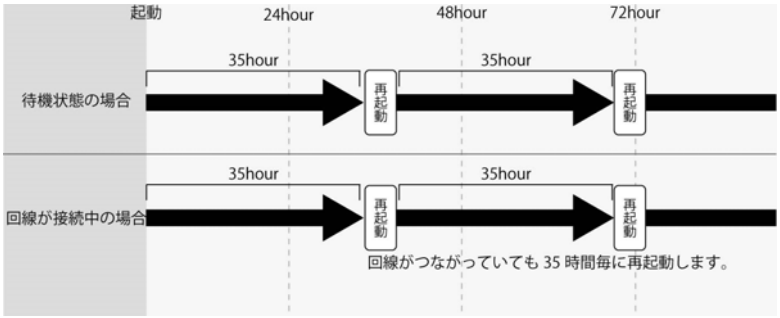
1. ハードウェア

ハードウェア上でRooster-RW Pro本体をリセットさせるための設定です。
「35時間毎」、「6日毎」、「使用しない」のいずれかを選択します。

メモ	ソフトウェアの設定が何等かの影響にて動作しなかった時の保険的な機能です。

注意	回線がつながった状態でも、設定時間になるとハードウェアが再起動します、 ハードウェアの設定時間は目安ですので、実際の動作時間は多少前後します。

〈例〉
ハードウェア：35時間毎



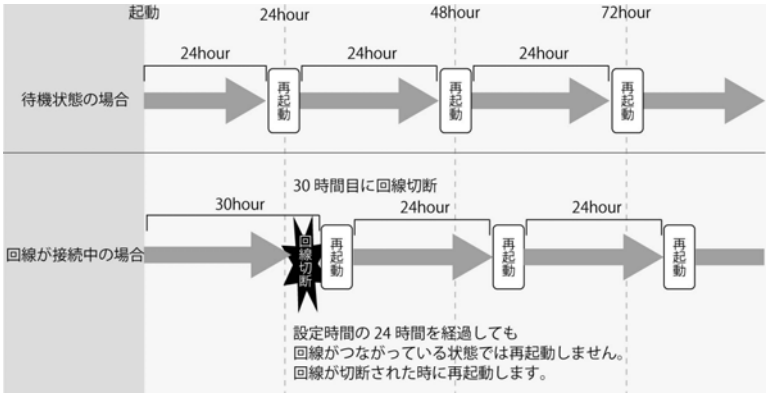
2. ソフトウェア

ソフトウェア上でRooster-RW Pro本体をリセットさせるための設定です。
使用する場合は「使用する」を選択し、「間隔」にリセットさせる間隔を入力してください。使用しない場合は「使用しない」を選択してください。

注意	設定時間時に回線がつながった状態では、ソフトウェアは再起動いたしません。 回線切断後に再起動します。

メモ	ダイヤルアップに 12 回連続して失敗すると、モバイルカードが再起動します。

〈例〉
ソフトウェア：使用する、1日毎

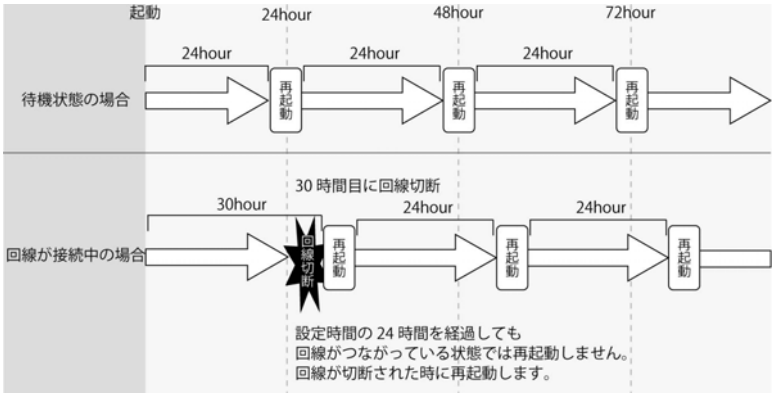


3. モバイルカード

モバイルカードを24時間毎にリセットさせるための設定です。
使用する場合は「使用する」を選択し、使用しない場合は「使用しない」を選択してください。

注意	設定時間時に回線がつながった状態では、モバイルカードは再起動いたしません。 回線切断後に再起動します。

〈例〉
モバイルカード：使用する



4. 選択した設定でよければ 設定 ボタンをクリックします。
   キャンセル をクリックすることで、設定を中止することができます。
5. 設定を反映させるためには、Rooster-RW Pro の電源を入れ直す必要があります。
   AC アダプタを抜き差しする等をおこなってください。

資料1

- **遮断ログ**

ファイアウォールが検出した不正なパケットの情報は「遮断ログ」に記録されます。
このろぐに表示されるパケットはRooster-RW Proが破棄するので、外部ネットワークにも内部ネットワークにも流れません。

Port Filter Defense
接続しようとしたポートはフィルタリングされています。 このポートを使ったアプリケーションを使用する場合は「高度な設定」の「フィルタリング」で設定してください。
Default Defense
ファイアウォールのデフォルト設定で接続が禁止されています。
Disallowed Destination IP
送信先の IP アドレスにはパケットを送信出来ません。
Invalid IP Packet Size
パケットヘッダのサイズが誤っています。
Black List Defense
送信元の IP アドレスはブラックリストに登録されています。ブラックリストは動的に作られます。
Invalid Configuration
NAT を使用する設定になっているにもかかわらず、グローバルネームスペースがありません。
No Existing Session
対応するセッションがありません。
No Enough Resources
Rooster のメモリ不足でセッションが確立できません。

資料2

■ Rooster-RW Pro のファイアウォール

Rooster-RW Proは以下のようなサービス拒否（Dos）攻撃やスキャンを検出してブロックするファイアウォール機能を持ちます。

● **サービス拒否（DoS）攻撃**

SynFlood

大量の接続要求パケット（SYN パケット）を送信することで相手サーバに過剰な負荷をかけるサービス拒否（DoS）攻撃です。

andAttack

TCP 接続要求パケット（SYN パケット）を偽造して、送信元 IP アドレスとポート番号の両方を送信先と同一にするという方法で、相手サーバが無限ループに陥ることを狙ったサービス拒否（DoS）攻撃です。

LWinNuke

NETBIOS ポート（139）に帯域外通知（OOB）データを送ることで相手サーバをダウンさせようとする攻撃です。Windows95 だけが影響を受けます。

Smurf

Ping パケットの送信元 IP アドレスを攻撃対象の IP アドレスに偽装して、ブロードキャストとして送信します。この結果、攻撃対象のサーバはネットワーク上のすべてのマシンから Ping 応答を受け取ることになり過負荷状態に陥ります。

Boink

TCP/IP パケットのフラグメントオフセットを改竄して相手サーバが分割されたパケットを再構築する際に巨大すぎて扱えないようにするサービス拒否（DoS）攻撃です。

IcmpFlood

大量の ICMP パケットを送って、サーバやネットワークに過剰な負荷をかけるサービス拒否（DoS）攻撃です。

Ascendkill

ASCEND 社ネットワーク機器は UDP ポート 9（Discard）を使ったリモートメンテナンス機能を持つ機種があります。この機能を悪用したサービス拒否（DoS）攻撃です。

EchoStorm

ICMP エコーサービスを悪用したサービス拒否（DoS）攻撃です。大量の ECHO パケットを送って相手サーバやネットワークに過剰な負荷をかけます。

Jolt

フラグメントされた巨大なパケットを受け取るとWindows95 がハングアップするという問題を悪用したサービス拒否（DoS）攻撃です。

OverDrop

Linux2.0 のあるバージョンはフラグメントされたパケットを受け取ると IP モジュールのデバック用メッセージを出力するものがあります。このとき、巨大なパケットを受け取るとメモリフォルトを発生することがあります。この問題を悪用したサービス拒否（DoS）攻撃です。

PingOfDeath

規定サイズ以上の大きさの Ping パケットを送って、相手サーバをクラッシュさせるサービス拒否（DoS）攻撃です。

EchoChargen

ネットワークの動作や性能を目的に用意されている 2 つのサービスを組み合わせて、故意に大量のトラフィックを発生させるサービス拒否（DoS）攻撃です。UDP パケットを偽装して、相手サーバの Chargen ポート向けに Echo ポートからのパケットを送ります。Chargen サービスはランダムな文字列を送信元に返すサービスなので、偽装された自身の Echo ポートに文字列を送信します。Echo サービスはその文字列をまた Chargen ポートに送り返すため無限ループとなり過大な負荷が発生します。

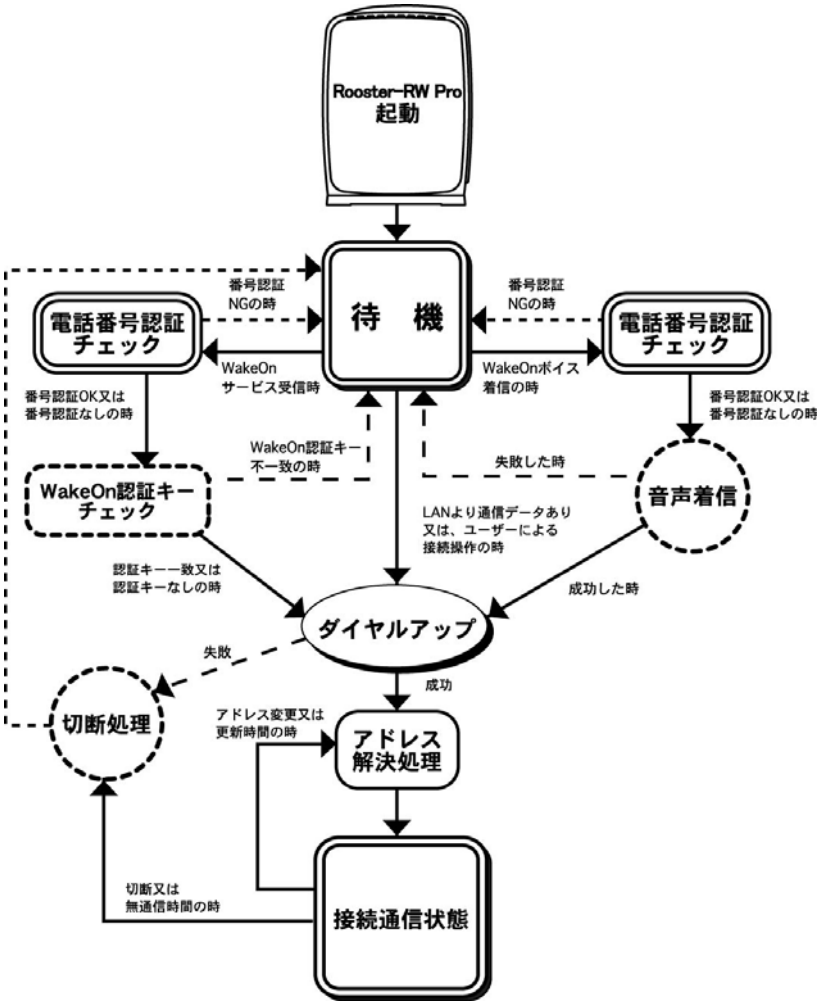
- **ポートスキャン**

ImapSynFinScan
IMAP ポートのスキャンです。古いバージョンの IMAP はセキュリティの脆弱性が報告されているのでそれを悪用したクラッキングを行おうとする者がスキャンをしている可能性があります。
UdpEchoScan
EchoChargen など UDP の Echo サービスを悪用しようとする者が UDP Echo ポートのスキャンを行っている可能性があります。
ChargenScan
EchoChargen など Chargen サービスを悪用しようとする者が Chargen ポートのスキャンを行っている可能性があります。
TcpSynAckScan
TCP パケットの SYN フラグを悪用したポートスキャンの手法です。ポートが開いているかを調べます。SYN を送って SYN/ACK が帰ってくるか、それとも RST/ACK が帰ってくるかをみることで、ポートの状態を知ります。
TcpFinScan
TCP パケットの FIN フラグを悪用したポートスキャンの手法です。ポートが開いているかを調べます。FIN を送って RST が帰ってくるかをみることでポートの状態を知ります。
TcpResetScan
全ての TCP フラグを“0”にするスキャン手法です。ポートが開いているかを調べます。FIN を送って RST が帰ってくるかをみることでポートの状態を知ります。
XmasTree
全ての TCP フラグを“1”にするスキャン手法です。ポートが開いているかを調べます。FIN を送って RST が帰ってくるかをみることでポートの状態を知ります。
BackOrificeScan
BACK ORIFICE（トロイの木馬）が仕掛けられていないかどうかを調べるスキャンです。
NetBusScan
Net Bus（トロイの木馬）が仕掛けられていないかどうか調べるスキャンです。

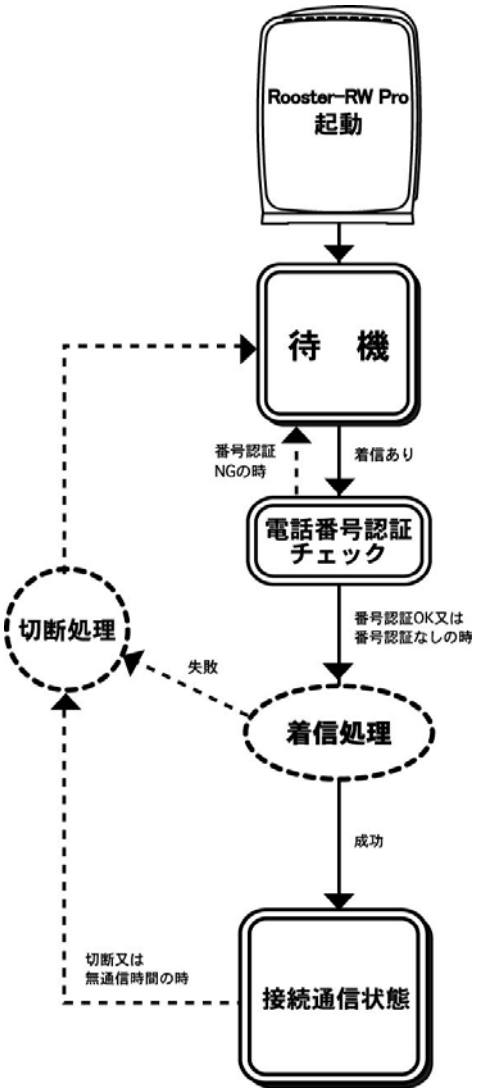
資料3

モバイルカード動作フロー図

- **「ダイヤルアップとして使用する」と設定した場合**



- **「RAS として使用する」と設定した場合**

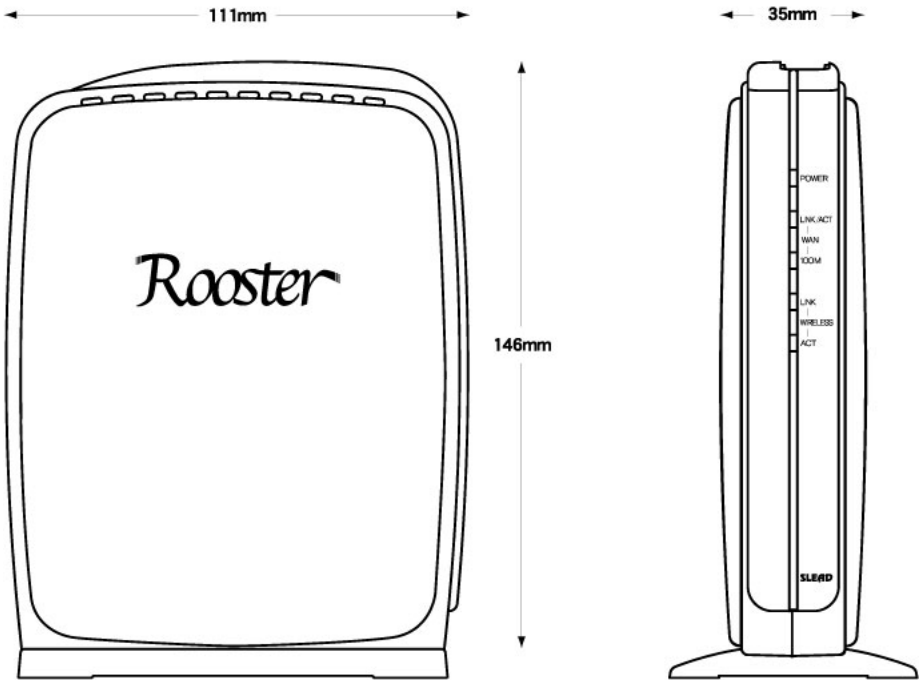


製品仕様

製品名		Rooster-RW Pro
型名		SC-RS601GK
JAN コード		4582131720171
ルーティング方式		スタティックルーティング （デフォルトルートのみ）
インターフェイス		MDI/MDI-X 自動判別
	LAN ポート	100BASE-TX/10BASE-T ×4 ポート
	WAN ポート	100BASE-TX/10BASE-T ×1 ポート
	PCMCIA ポート	TypeⅡ準拠(3.3/5V 両対応) ×1 ポート
ハードウェア構成	CPU	MIPS CORE
	メインメモリ	8MB
	フラッシュメモリ	1MB
リセットスイッチ		1 個
電源仕様		AC アダプタ
	定格入力	AC100V (50/60Hz)
	定格出力	DC12V 1.0A
	最大消費電力	7.5W
環境条件	温度	5～40℃
	湿度	25～85%(結露なきこと)
	耐ノイズ性 AC ラインノイズ DC ラインノイズ	±2000V パルス幅 100ns/1000ns ±2000V パルス幅 100ns/1000ns ノイズシュミレータによる ※非フェライトコア接続時
	耐静電気性 直接放電 気中放電	±10KV LAN 端子金属部 ±10KV LAN 端子金属部
重量		約 207g(付属品含まず)
外形寸法		35(W)×146(H)×111(D)mm (付属物/ケーブル/突起物は含まず)
サポートプロトコル	Ethernet	CSMA/CD
	ルーティング	IP のみ
	WAN	PPPoE 同時セッション 1
	認証	PAP、CHAP
	ダイヤルアップ	PPP
DHCP		サーバ機能(LAN 側最大 253 クライアント) クライアント機能（WAN ポートのみ）
アドレス変換		NAT/IP マスカレード
VPN パススルー		IPsec/PPTP パススルー（1 セッション）
サーバ公開		バーチャルサーバ(最大 12 件設定可) DMZ ホスト(1 件設定可)
アップデート		WWW ブラウザによるアップデート
WakeO 着信	メッセージ認証登録	メッセージ登録(128 文字)/1 件
	着信番号登録	CLID/16 件

リモートアクセス	プロトコル	PIAFS2.2/2.1/2.0/1.0/FOMA64K （モバイルカードに依存）
	認証方式	PAP、CHAP、CLID×50 件
モバイルカード情報表示(対応モバイルカードのみ)		自局電話番号/電界強度/位置情報
FOMA LAN 接続		オープン接続、クローズ接続
アドレス解決	アドレス登録	1 件
	メッセージ登録	1 件
	プロトコル	SMTP、POP
	ダイナミック DNS	どこでもカメラ、DynDNS
	更新時間設定	可能 (5 分～)
WAN ハートビート	相手先	WAN ゲートウェイ
	更新時間設定	可能 (1 分～)
無通信監視タイマー		設定可能
電源制御		ハードウェア及びソフトウェア　モバイルカード ※本体電源 OFF から 10 秒±5 秒で電源 ON
ハードウェアウォッチドック 信号受信タイミング 発動条件 発動動作		常時監視(1 秒毎) 信号不受信から約 1 分 30 秒後 本体電源 OFF から 10 秒後に再起動
ダイヤルアップ自動発信条件		LAN 側からのパケット送出　WAN ハートビート
ダイヤルアップ手動発信/切断		可能
ダイヤルアップ先設定		1 件
ロギング		WWW ブラウザによる各種ログ表示
		● パケット通信ログ ● パケット遮断ログ ● モバイルカードログ ● アドレス解決ログ ● WAN ハートビートログ
パケットフィルタリング		最大 36 件登録可能 以下の各パラメータによるフィルタリング プロトコル番号またはポート番号、プロトコル、方向
ファームウェア設定		WWW ブラウザによる設定
インターネット経由の リモートセットアップ		可能（WWW ブラウザ）
保証		1 年間
付属品		CD-ROM(取扱説明書類収録) ---1 枚 保証書---1 枚 AC アダプタ---1 個 UTP ケーブル(カテゴリ 5 ストレート)---1 本 縦置きスタンド---1 個 カードスロットフタ---1 個

外形寸法



付属品・突起物含まず：単位 mm

サポートのご案内

- **最新情報の入手**

  Rooster-RW Proに関する最新情報は、弊社ホームページから入手することができます。また、バージョンアップ情報につきましても公開しております。

  ■ **製品紹介ページ**

  http://www.sun-denshi.co.jp/sc/rooster_rwpro/

- **ご質問・お問い合わせ**

  Rooster-RW Proに関するご質問やお問い合わせは、下記へご連絡願います。

サン電子株式会社　サンコミュニケーションズ事業部　サポートセンター	
電話	0587-55-0161
FAX	0587-55-0815
メール	support-suncomm@sun-denshi.co.jp
受付時間	月曜～金曜　10:00～16:00(12:00～13:00 を除く) 祝祭日、弊社休日を除く

Rooster™-RW Pro
SC-RS601GK
取扱説明書　Ver.1.4

2009 年 6 月発行

サン電子株式会社
〒483-8555　愛知県江南市古知野町朝日 250
※無断複写・転載を禁止します。

(090610)